



(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
29.04.2009 Bulletin 2009/18

(51) Int Cl.:
G07F 7/10 (2006.01) G06F 21/00 (2006.01)

(21) Numéro de dépôt: **07301410.2**

(22) Date de dépôt: **28.09.2007**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL BA HR MK RS

(71) Demandeur: **GEMPLUS**
13420 Gémenos (FR)

(72) Inventeurs:
• **Amiel, Frédéric**
CARNOUX 13470 (FR)
• **Gauteron, Laurent**
MARIGNANE 13700 (FR)

(54) **Procédé de génération de masques dans un objet communiquant et objet communiquant correspondant**

(57) L'invention concerne un procédé de génération de masques dans un objet communiquant, les masques étant destinés à masquer des données à stocker dans l'objet communiquant. Au moins un masque maître (11) est stocké dans l'objet communiquant.

Selon l'invention, le procédé consiste à :

- appliquer au moins un diversifiant (D) au masque maître (11), de manière à générer un masque diversifié (14) ;
- masquer par une fonction réversible (12) la donnée (10)

à stocker dans l'objet communiquant à l'aide du masque diversifié (14), le masquage générant une donnée masquée (15) ;

- stocker la donnée masquée (15) dans l'objet communiquant avec le diversifiant (D) ayant servi à générer le masque diversifié (14) ayant permis d'obtenir la donnée masquée (15).

L'invention concerne également un objet communiquant comprenant des moyens mettant en oeuvre un tel procédé.

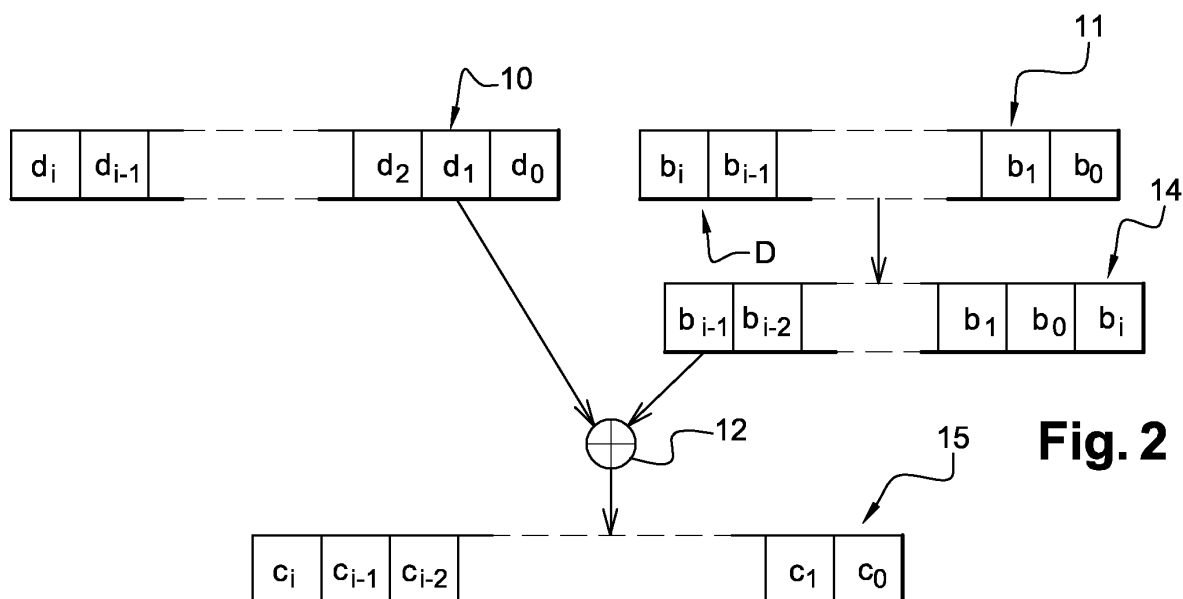


Fig. 2

Description

[0001] Le domaine de l'invention est celui des objets communicants, tels que notamment les cartes à puce, les téléphones mobiles ou les PDAs. Plus précisément, la présente invention concerne un procédé de génération de masques dans un objet communicant.

[0002] Dans la suite de cette description, on appellera « masque » une fonction numérique destinée à masquer une donnée sensible ou des instructions d'un programme que l'on désire garder secrète dans l'objet communicant. Dans le domaine de la carte à puce, une telle donnée est par exemple une clé, un code, un identifiant du propriétaire de la carte ou alors un algorithme ou des instructions que l'on ne souhaite pas divulguer à un attaquant éventuel. Ces données ne sont donc pas stockées « en clair » dans la carte.

[0003] Afin de masquer une donnée sensible dans une carte à puce, il est connu d'appliquer une fonction mathématique à cette donnée sensible. La donnée résultante est alors une donnée masquée qui est stockée dans la mémoire de la carte. Ultérieurement, si l'on souhaite lire cette donnée sensible, une fonction mathématique inverse de la précédente est appliquée à la donnée masquée et la donnée sensible peut alors être récupérée pour son utilisation, par exemple pour l'exécution d'un programme.

[0004] La fonction mathématique est par exemple un Ou-Exclusif.

[0005] La figure 1 représente le masquage d'une donnée 10 comprenant i octets d_0 à d_i . Le masque utilisé pour masquer la donnée 10 est noté 11 et comporte également i octets b_0 à b_i . La fonction de masquage est ici une fonction Ou-exclusif 12. La donnée masquée est notée 13 et comporte i octets c_0 à c_i , avec $c_i = d_i \oplus b_i$. Le masquage consiste donc à réaliser un Ou-exclusif orienté octet.

[0006] En appliquant le masque 11 à la donnée masquée 13 par la fonction Ou-exclusif, on régénère la donnée 10, la fonction Ou-exclusif étant réversible.

[0007] L'inconvénient de cette solution connue est qu'il est possible à un attaquant de retrouver le masque 11 en injectant des fautes dans l'objet communicant, par exemple une carte à puce, ou en exploitant des dysfonctionnements de celui-ci. Ces attaques sont également appelées des attaques par « dump » en anglais. Si le masque 11 est révélé à l'attaquant, celui-ci pourra sans difficulté particulière lire l'ensemble des données masquées mémorisées dans l'objet communicant.

[0008] Une solution pour pallier à cet inconvénient lié à la présence d'un masque unique est de prévoir plusieurs masques dans l'objet communicant et de changer de masque en fonction de l'application ou du type de donnée à masquer. Cette solution présente néanmoins l'inconvénient de nécessiter la mémorisation de plusieurs masques dans l'objet communicant, ce qui n'est guère envisageable lorsque la ressource mémoire est petite, ce qui est le cas des cartes à puce.

[0009] La présente invention a pour objectif de remédier à cet inconvénient.

[0010] Plus précisément, un des objectifs de l'invention est de proposer un procédé de masquage de données pour objet communicant permettant de masquer un nombre très important de données sans nécessiter de mémorisation de plus d'un masque ou tout du moins d'un nombre de masques important.

[0011] Cet objectif, ainsi que d'autres qui apparaîtront par la suite, est atteint grâce à un procédé de génération de masques dans un objet communicant, les masques étant destinés à masquer des données à stocker dans l'objet communicant, au moins un masque maître étant stocké dans l'objet communicant, le procédé consistant à :

- appliquer au moins un diversifiant au masque maître, de manière à générer un masque diversifié ;
- masquer par une fonction réversible la donnée à stocker dans l'objet communicant à l'aide du masque diversifié, le masquage générant une donnée masquée ;
- stocker la donnée masquée dans l'objet communicant avec le diversifiant ayant servi à générer le masque diversifié ayant permis d'obtenir la donnée masquée.

[0012] L'application de diversifiants au masque maître permet ainsi d'obtenir des masques diversifiés qui sont utilisés pour masquer les données.

[0013] De préférence, la fonction réversible utilisée est une fonction Ou-Exclusif.

[0014] Avantageusement, l'application d'un diversifiant au masque maître consiste à appliquer une rotation au masque maître. Ainsi, la génération de masques diversifiés consiste en de simples rotations du masque maître. Pour un masque maître de 256 octets, il sera donc possible de générer 256 masques différents si la rotation est orientée octets. Il est bien entendu également possible d'effectuer des rotations au niveau bit, ce qui augmente encore le nombre de masques différents pouvant être générés.

[0015] Le diversifiant est de préférence généré de manière pseudo-aléatoire dans l'objet communicant. Ceci présente l'avantage de pouvoir masquer les données à la volée.

[0016] Avantageusement, les masques maîtres sont diversifiés d'un objet communicant à un autre. Ainsi, même si un attaquant réussit à découvrir le masque maître d'un objet communicant, il ne pourra pas démasquer les données mémorisées dans un autre objet communicant puisque leurs masques maîtres sont différents.

[0017] L'invention concerne également un objet communicant comprenant des moyens de mise en oeuvre d'un tel procédé.

[0018] L'objet communicant consiste préférentiellement en une carte à puce.

[0019] D'autres avantages et caractéristiques de la

présente invention apparaîtront à la lecture de la description suivante d'un mode de mise en oeuvre préférentiel, donné à titre illustratif et non limitatif, et des dessins annexés, dans lesquels :

- la figure 1 représente le principe de masquage d'une donnée, conformément à l'état de la technique ;
- la figure 2 représente un mode de mise en oeuvre préférentiel du procédé selon l'invention.

[0020] La figure 1 a été décrite précédemment en référence à l'état de la technique.

[0021] La figure 2 représente un mode de mise en oeuvre préférentiel du procédé selon l'invention.

[0022] Dans ce mode de mise en oeuvre préférentiel, un masque 11, appelé masque maître, est utilisé. Le masque maître 11 est mémorisé dans l'objet communiquant. L'invention propose d'appliquer un diversifiant D au masque maître 11 afin de générer un masque diversifié 14.

[0023] Dans un mode de mise en oeuvre préférentiel, le diversifiant D est un simple pointeur qui marque l'octet du masque maître 11 qui sera utilisé pour masquer le premier octet de la donnée 10. Sur la figure 2, le diversifiant D pointe sur l'octet b_{i-1} et c'est donc cet octet qui sera le premier du masque diversifié. Les autres octets sont pris les uns à la suite des autres, dans un mode de mise en oeuvre simplifié. On obtient ainsi, un masque diversifié 14 dont le premier octet est b_{i-1} et le dernier octet est b_i . On aura donc simplement appliqué une rotation aux octets du masque maître 11. Il est également possible d'appliquer des rotations aux bits du masque maître 11, la rotation étant alors orientée bits.

[0024] Ensuite, les octets d_0 à d_i de la donnée 10 sont masqués à l'aide des octets du masque diversifié 14 pour fournir la donnée masquée 15.

[0025] Afin de pouvoir démasquer la donnée masquée 15, celle-ci est stockée dans l'objet communiquant avec le diversifiant D qui a servi à générer le masque diversifié 14, c'est-à-dire avec le diversifiant ayant permis de l'obtenir. La donnée masquée 15 est de ce fait associée au diversifiant D.

[0026] Lors de l'écriture ou de la création d'une autre donnée dans la carte, un autre diversifiant sera généré, de préférence de manière aléatoire, afin de générer un autre masque diversifié qui servira au masquage de cette autre donnée.

[0027] L'avantage de l'invention est qu'il est possible de générer autant de masques diversifiés qu'il y a d'octets (ou de bits) dans le masque maître 11. Le stockage du diversifiant D est peu gourmand en place mémoire, typiquement un octet.

[0028] Afin de renforcer la sécurité du procédé selon l'invention, il est possible d'utiliser plus d'un masque maître, par exemple deux, et de générer deux diversifiants D1 et D2. Le diversifiant D1 sera appliqué au premier masque maître et le diversifiant D2 au second masque maître. Chaque octet d'une donnée à masquer sera mas-

qué, par exemple à l'aide de la fonction Ou-exclusif, par un octet du premier masque diversifié et par un octet du second masque diversifié. Les diversifiants D1 et D2 seront alors stockés avec la donnée masquée. Pour un masque maître de 256 octets, il est alors possible de générer 256^2 masques différents.

[0029] L'invention s'applique particulièrement bien dans un environnement Java, les diversifiants pouvant être stockés avec l'entête des objets Java.

[0030] La fonction réversible Ou-Exclusif n'est pas la seule qui puisse être employée : il est possible d'utiliser une fonction DES ou alors une simple rotation. Toute fonction réversible convient à l'invention.

[0031] Le diversifiant D est de préférence généré aléatoirement ou pseudo-aléatoirement lorsque la donnée 10 est inscrite/crée dans l'objet communiquant ou à chaque redémarrage de l'objet communiquant.

[0032] D'un objet communiquant à un autre, les masques maîtres 11 sont de préférence diversifiés. Ceci assure qu'en cas d'attaque réussie sur un objet communiquant, l'attaquant en possession d'un masque maître ne puisse démasquer les données masquées dans un autre objet communiquant.

[0033] L'invention s'applique à tout objet communiquant, tel que par exemple aux téléphones portables et préférentiellement aux cartes à puce, par exemple aux cartes à puce multi-applicatives.

30 Revendications

1. Procédé de génération de masques (14) dans un objet communiquant, lesdits masques (14) étant destinés à masquer des données (10) à stocker dans ledit objet communiquant, au moins un masque maître (11) étant stocké dans ledit objet communiquant, ledit procédé consistant à :

- appliquer au moins un diversifiant (D) audit masque maître (11), de manière à générer un masque diversifié (14) ;
- masquer par une fonction réversible (12) ladite donnée (10) à stocker dans ledit objet communiquant à l'aide dudit masque diversifié (14), ledit masquage générant une donnée masquée (15) ;
- stocker ladite donnée masquée (15) dans ledit objet communiquant avec le diversifiant (D) ayant servi à générer le masque diversifié (14) ayant permis d'obtenir ladite donnée masquée (15).

2. Procédé selon la revendication 1, **caractérisé en ce que** ladite fonction réversible est une fonction Ou-Exclusif (12).

3. Procédé selon l'une des revendications 1 et 2, **caractérisé en ce que** ladite application d'un diversi-

fiant (D) audit masque maître (11) consiste à appliquer une rotation audit masque maître (11).

4. Procédé selon l'une des revendications 1 à 3, **caractérisé en ce que** ledit diversifiant (D) est généré de manière pseudo-aléatoire dans ledit objet communiquant. 5
5. Procédé selon l'une des revendications 1 à 4, **caractérisé en ce que** les masques maîtres (11) sont diversifiés d'un objet communiquant à un autre. 10
6. Objet communiquant comprenant des moyens de mise en oeuvre d'un procédé selon l'une des revendications 1 à 5. 15
7. Objet communiquant selon la revendication 6, **caractérisé en ce qu'il** consiste en une carte à puce. 20

20

25

30

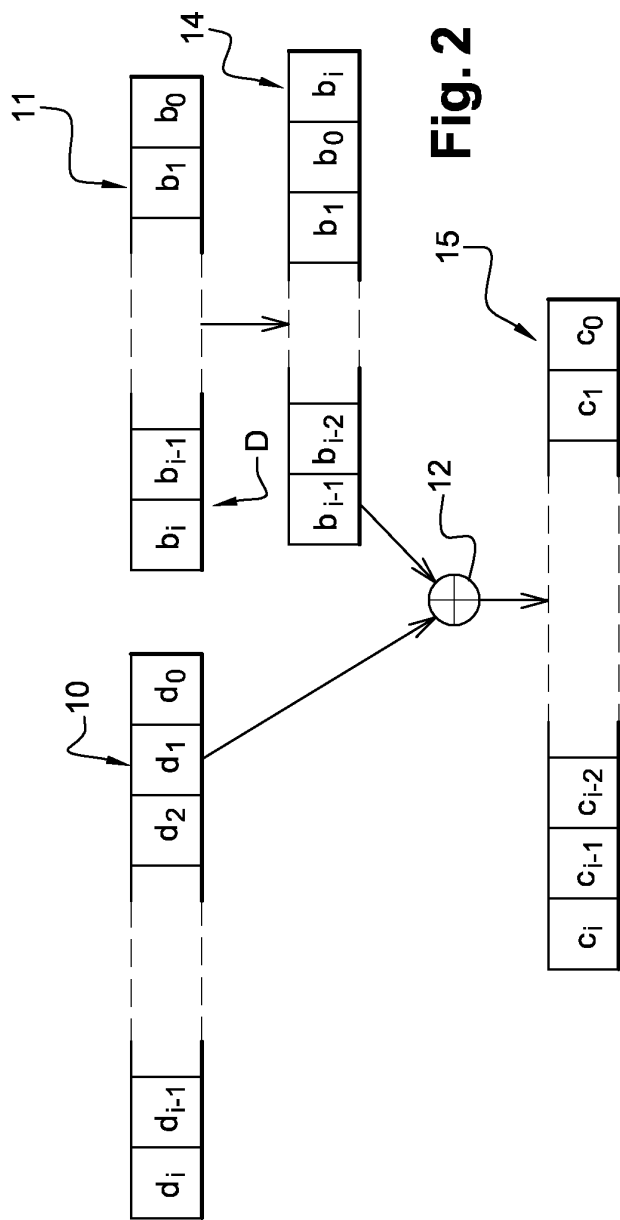
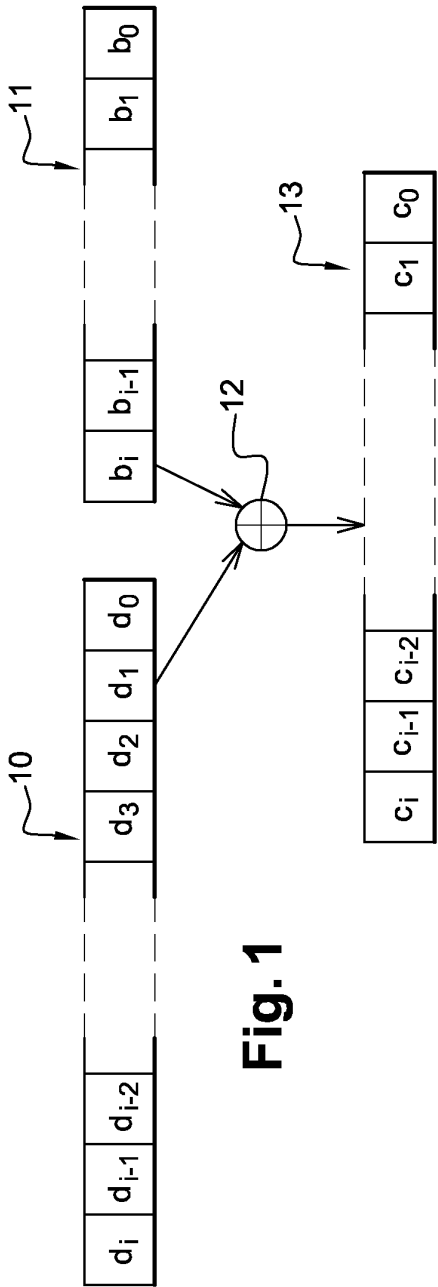
35

40

45

50

55





DOCUMENTS CONSIDERES COMME PERTINENTS			
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
X	GB 2 264 373 A (EUROLOGIC RESEARCH LIMITED [IE]) 25 août 1993 (1993-08-25) * le document en entier *	1-7	INV. G07F7/10 G06F21/00
A	DE 103 44 636 A1 (INFINEON TECHNOLOGIES AG [DE]) 25 mai 2005 (2005-05-25) * le document en entier *	1-7	
A	US 2003/070083 A1 (NESSLER KAI-WILHELM [NO]) 10 avril 2003 (2003-04-10) * le document en entier *	1-7	
A	US 2007/067644 A1 (FLYNN WILLIAM T [US] ET AL) 22 mars 2007 (2007-03-22) * le document en entier *	1-7	
A	US 5 428 685 A (KADOOKA YOSHIMASA [JP] ET AL) 27 juin 1995 (1995-06-27) * le document en entier *	1-7	
A	US 2007/223705 A1 (KASAHARA AKIHIRO [JP] ET AL) 27 septembre 2007 (2007-09-27) * le document en entier *	1-7	DOMAINES TECHNIQUES RECHERCHES (IPC) G07F G06F
Le présent rapport a été établi pour toutes les revendications			
Lieu de la recherche La Haye		Date d'achèvement de la recherche 18 mars 2008	Examineur Guenov, Mihail
CATEGORIE DES DOCUMENTS CITES X : particulièrement pertinent à lui seul Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie A : arrière-plan technologique O : divulgation non-écrite P : document intercalaire T : théorie ou principe à la base de l'invention E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date D : cité dans la demande L : cité pour d'autres raisons & : membre de la même famille, document correspondant			

2

EPO FORM 1503 03.82 [P04C02]

**ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE
RELATIF A LA DEMANDE DE BREVET EUROPEEN NO.**

EP 07 30 1410

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.

Lesdits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du

Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

18-03-2008

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
GB 2264373	A	25-08-1993	AUCUN	
DE 10344636	A1	25-05-2005	AUCUN	
US 2003070083	A1	10-04-2003	AUCUN	
US 2007067644	A1	22-03-2007	AUCUN	
US 5428685	A	27-06-1995	WO 2004077300 A1	10-09-2004
US 2007223705	A1	27-09-2007	CN 1977490 A	06-06-2007
			JP 2006014035 A	12-01-2006
			WO 2006001161 A1	05-01-2006

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82